



referentia



# PMRF Force Protection Lab (PFPL) Phase I ONR Contract N00014-06-C-0107 Industry Day Presentation

April 26, 2006

David C. Brauer  
Program Manager  
Referentia Systems Inc.





## Presentation Outline

- Introduction
- Technology Survey
  - Base Survey
  - Scenarios, Behaviors, Observables and MOEs
  - Security Technology Survey
- Baseline Model
  - Demo of PMRF Base Protection Lab (PBPL) Security Benchmarking Tool (SBT)
  - Sample Output
- Baseline Architecture
- Baseline Effects
- Recommended Investment Priorities



## Introduction - Background

- Prior to 9/11...
  - Open access to recreational areas on base
  - Hosting of special events
- Since 9/11...
  - Significantly reduced open access
  - Adverse impact/hardship for civilians
  - Significant advances in security technology (Homeland Security and Force Protection)
- So...
  - Apply these technology advances to re-open access to bases while preserving safety, security and mission



## Introduction - PBPL Purpose and Scope

- Provide a realistic testbed environment
  - Develop, integrate, test and evaluate promising security technologies
  - Determine “best of breed” solutions
  - Leverage diverse base environment without affecting critical base missions or assets
- Not intended as a new security system for PMRF, must not compromise security
- But... over time will transition tested, best-of-breed, leading-edge technologies to PMRF Base Security

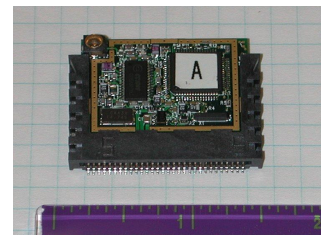


## Introduction - PBPL Outcomes

- Provide new solutions for open-access base security leveraging advanced sensors, situational awareness, behavior analysis, etc.
- Position the PMRF Base Protection Lab at the leading edge of open-access base security R&D, testing and evaluation



Vigilante VTOL UAV



Advanced Sensors



EO/IR Sensors



## Technology Survey

- PMRF Base Survey
  - Tour base and view current facilities
  - Discuss current security challenges
  - Understand normal base operations and flow
- Scenarios, Behaviors, Observables and Measures of Effectiveness
  - 5 Threat Scenarios
    - VBIED and Hostage, Suicide Bomber, Insider Theft, Vandalism and Event Disruption, Stealthy ED/CB Placement
  - Timelines with activities and observables
  - Detection requirements and MOEs
- Security Technology Survey





## Sample Scenario – Vandalism and Mission Event Disruption

### T- hrs to min

- 4-6 boats conduct diversion/harassment operations from offshore
- Signs, loudspeaker announcements, fireworks, etc. to create diversion
- Feints of illegal landings on beach, residential area, airfield

### T- 10 min

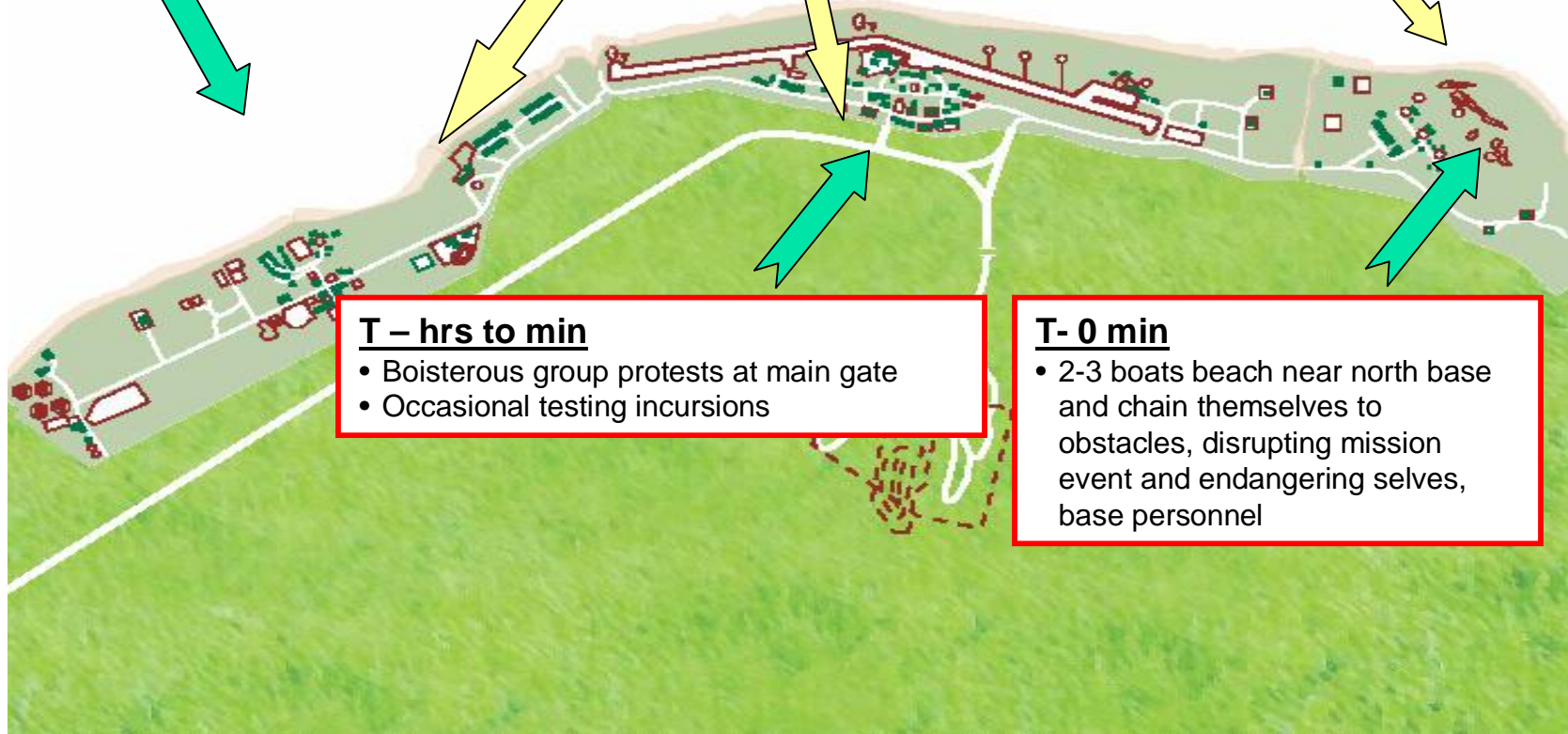
- 2-3 boats split off at high speed for north base
- Other boats beach at residential area
- Gate protestors surge past guards and vandalize nearby buildings

### T – hrs to min

- Boisterous group protests at main gate
- Occasional testing incursions

### T- 0 min

- 2-3 boats beach near north base and chain themselves to obstacles, disrupting mission event and endangering selves, base personnel





## Sample Scenario – Vandalism and Mission Event Disruption

### Possible Pre-Event Observables, Human Activity (Assume all Outsiders)

#### **External Information Sources**

- Local law enforcement, Mass media
- HUMINT by installation personnel
- Good Samaritan Reports By Locals
- Tour operator reports

#### **Surveillance**

- Groups or small number of individuals that do not hide their affiliation or purpose attempt to observe base activity during normal business hours
- Groups or small number of individuals that do not hide their affiliation or purpose attempt to visit the base during normal business hours

Time: months to days

Pre-Event

#### **Planning, Preparation**

- Groups or individuals prepare for application to enter the base as a local resident
- Increased frequency of inquiries at the base security checkpoint/ building.
- Acquisition of materials for defacement/endangerment of base assets

#### **Rehearsal**

- Coordinated patterns of activity and movement outside perimeter
- Comms intercepts
- Visual evidence of demonstrations outside of the entry to the base





## Sample Scenario – Vandalism and Mission Event Disruption

### Information Sources

- Gate guards and portal ID systems
- Security cameras
- Incursion detection systems
- Underwater incursion detection systems

### Supporting Diversion

- Harassment incursions from water near public beach and at gate
- Numerous unsuccessful attempts to enter the base by multiple coordinated individuals
- Scantily clad ladies (and men) deployed to the beach in front of the base
- Groups try to breach through security check points on foot
- Massive incursion by people overwhelming the guard forces getting into the base perimeter running to nearby buildings for to vandalize and deface

### Action

- Chain selves to obstacles
- Disrupt mission event

Time: seconds to hours

Event

### Movement to Objective

- Boats depart diversion op, rapidly navigate to launch site, beach boats, run to Mission Event area
- Boat movement to north base area, beaching
- Persons running to mission event site



## Security Technology Survey

- Technologies analysis specifically guided by Scenarios, Behaviors, Observables and MOEs
- Seven categories of technology analyzed
  - Land Barriers with Contact/Proximity Sensing
  - Low-Profile Incursion Detection Systems
  - Badge, Portal and Tracking Systems
  - Biometric Authentication for Point Access
  - Explosive Detection Systems
  - Nuclear, Chemical, Biological Sensors
  - Water, Underwater Incursion Detection and Barrier Systems
- MOEs, MOPs developed for each category
- 1-2 representative systems and ROM for each



## Baseline Model - Demo of PBPL SBT

PFPL

File Edit Help

Toolbar

**Simulation**

- Environment
  - Demo Excursion-1
    - Demo Scenario-1
      - Civilians
        - Demo Civilian-1
      - Intruders
        - Demo Intruder-1
      - Demo Security Solution-1
        - Sensors
          - Explosives Sensor
          - Excessive Weight Sensor
          - Route Divergence Sensor
      - Security Solution Variations
      - Replicates

**Properties**

Costs: Fixed

Bandwidth Cost	0
CPU Cost	0
Storage Cost	0
Total Fixed Cost	0
Fixed Unit Cost	0

Characteristics


Behavior Detected	CARRYING_EXPLOSIVES
Coverage Width	2
False Alarm Rate	0
Probability of Detection	0.5

Costs: Recurring

Maintenance Cost	0
Operational Cost	0
Total Recurring Cost	0
Training Cost	0
Recurring Unit Cost	0

Name

Name	Explosives Sensor
------	-------------------

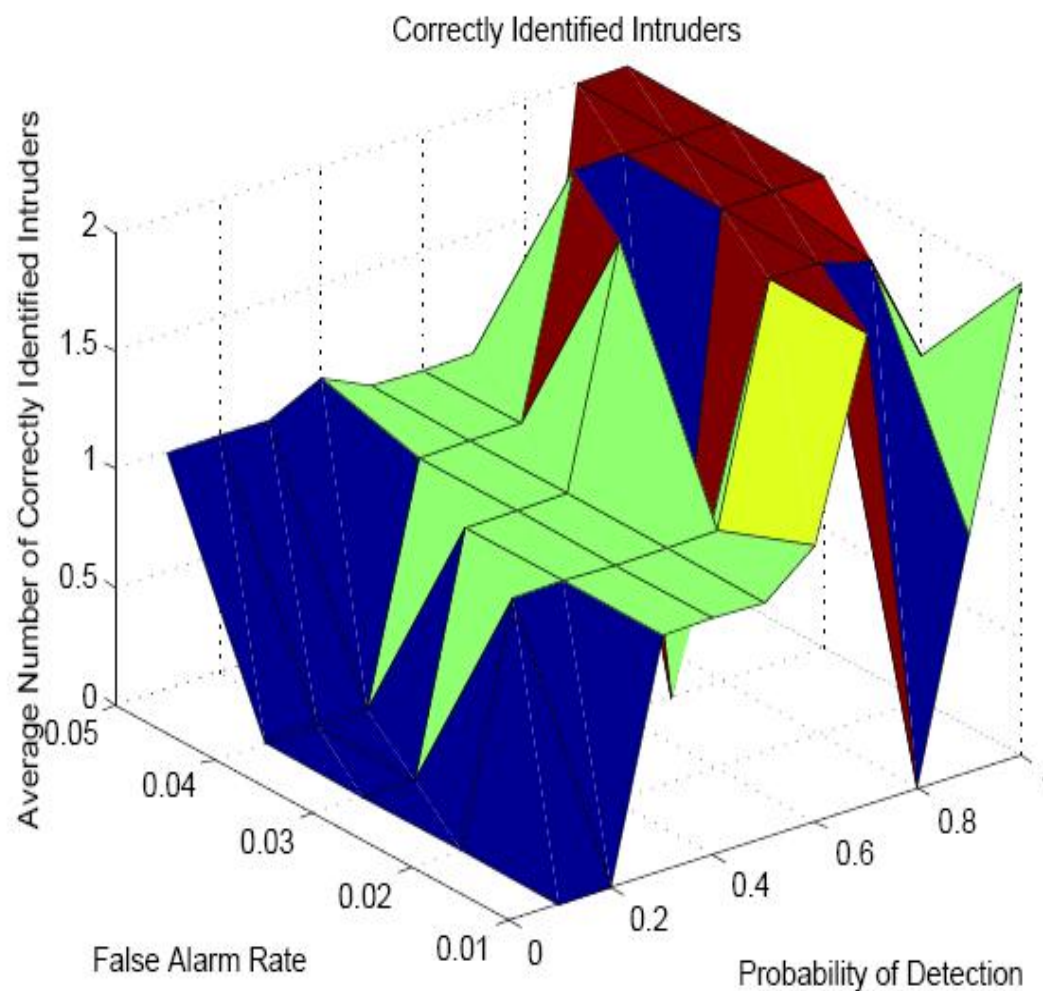


Behaviors Emitted | Behaviors Observed

Status:

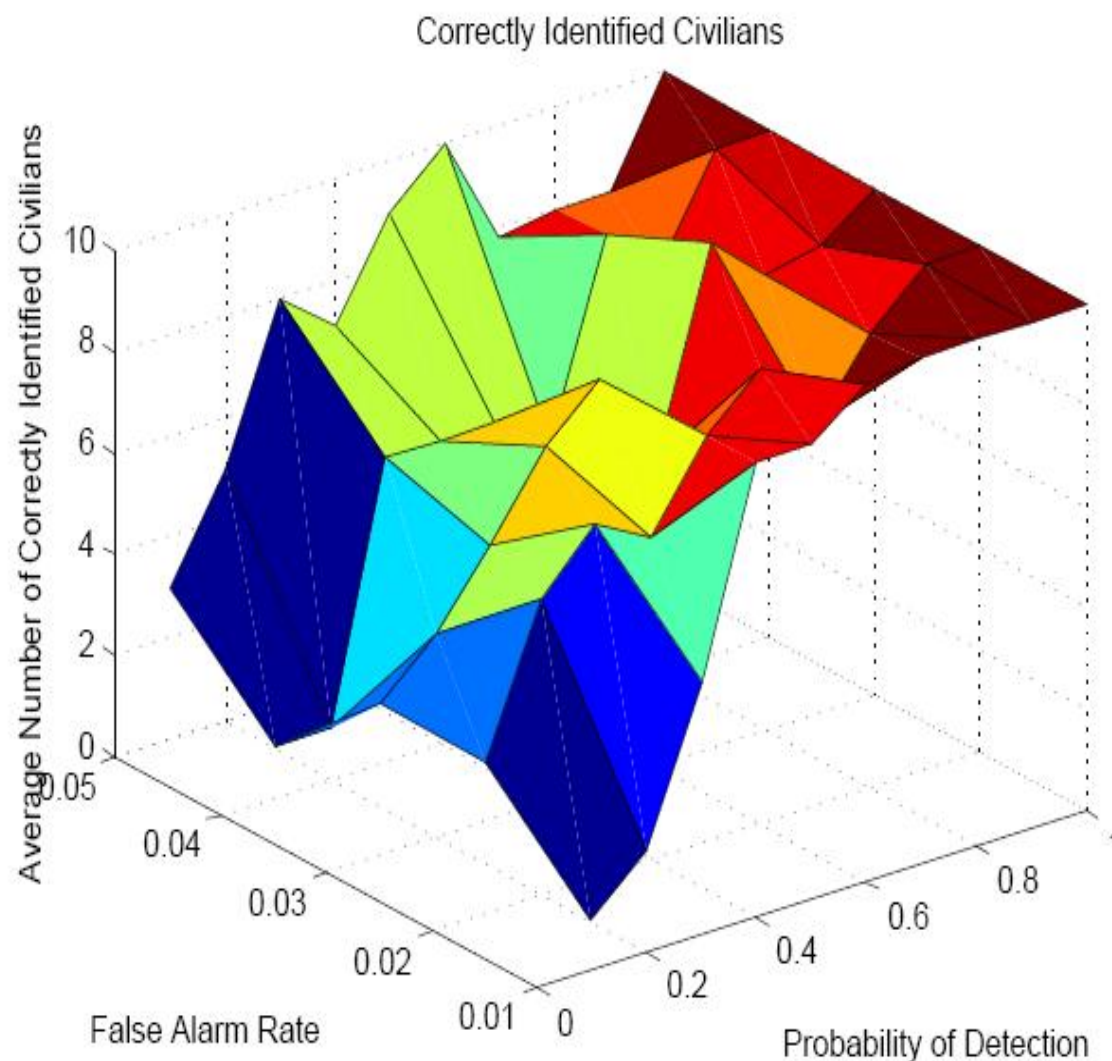


## Baseline Model - PBPL SBT Sample Output





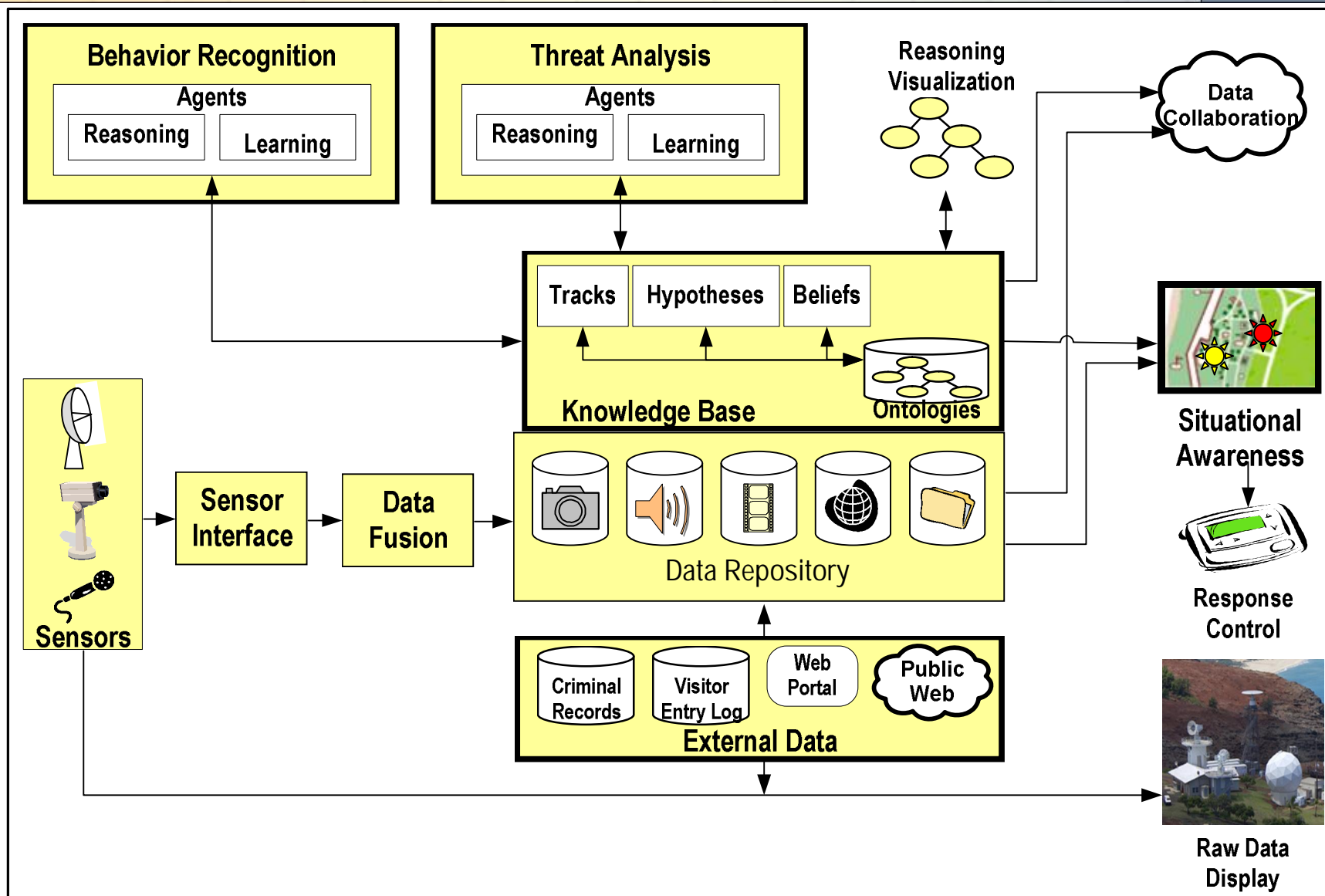
## Baseline Model - PBPL SBT Sample Output







## PBPL Baseline Architecture





## PBPL Baseline Architecture Key Features

- Inputs
  - Sensor data via common sensor interface and data fusion
  - External data for contextual knowledge
- Data and Knowledge Repository
  - Common database or tightly coupled
  - Ontologies express relationships between data, tracks, hypotheses and beliefs
- Cognitive Architecture
  - Agents can implement many approaches for reasoning and learning
  - Behavior Recognition and Threat Analysis are major functions
  - Reasoning Visualization allows human input to facilitate learning
- Outputs
  - Situational awareness displays alerts, warnings, tracks and security assets and guides response control
  - Situational awareness supports “zoom-in” to displayed elements to view raw and historical data
  - Data collaboration exports and redacts (where necessary) data and knowledge from the repository and makes it available as a Web service to remote researchers



## Baseline Effects

1. Pre-event and historical information establish the context for reasoning and learning
  - Law enforcement, base security, good Samaritan and other HUMINT
  - Comms intercepts and other SIGINT around base
  - Schedules and normal usage patterns on base
  - Relationships between observable behaviors
  - Examples:
    - Arrival/Settlement of potential hostile in area
    - Potential hostile seeking employment on base
    - Signs of insider cooperation with external agents
    - Information gathering about operations and vulnerabilities by external agents



2. Observed behaviors need to be associated with a time and location
  - Facilitates data fusion
  - Facilitates track formation and associated reasoning
  - Enriches historical information and supports learning
  - Examples:
    - Detection of a person in an “overwatch” position
    - Detection of movement across base perimeter
    - Unauthorized entry to secured area



## Baseline Effects

3. Primary behaviors, behaviors that are directly threatening, need prior context
  - Lead to an immediate conclusion of malicious intent
  - Tend to happen too late for a meaningful response
  - Are the focus of most available security technology
  - Examples:
    - Breaching fence or other perimeter demarcation
    - Carrying a weapon or explosive without authorization
    - Attempting unauthorized entry
    - Initiating a false alarm





## Baseline Effects

4. Secondary and tertiary behaviors can be correlated to lead to a conclusion of malicious intent
  - Requires algorithms/reasoning to correlate these behaviors
  - Tend to happen earlier in an event timeline
  - Examples of secondary behaviors
    - Speeding vehicle
    - Moving towards or in the vicinity of restricted area
  - Examples of tertiary behaviors
    - Diverging from authorized route



## Recommended Investment Priorities

- Development of a cognitive software architecture that establishes a context for reasoning and learning
- Development of standardized notations and ontologies for communicating about tracks, behaviors, hypotheses, beliefs and intent
- Intelligent agents implementing multiple techniques to reason about behaviors and threats and “learn” normal base activity
- Algorithms/reasoning to determine observed behaviors from raw and fused sensor data
- Algorithms/reasoning to determine malicious intent from observed behaviors

# A Notional Vision for PBPL



## Data Repository

- Stores sensor output
- Provides another level of linking/combination of sensors using various models
- Data types – video, time series, web pages, images, audio

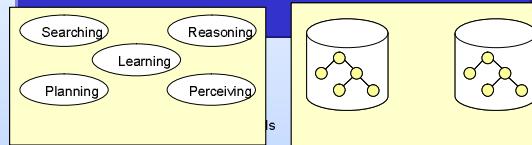
## Sensor Interface and Data Fusion

- Beam forming for acoustic/RF point sensors,
- Creating trajectories from sequences of point/area sensor outputs;
- Attributing id's (from access/biometric systems) to these aggregate sensor outputs or trajectories;
- Events from linking/combining multiple trajectories/fused sensor outputs.

Real time sensor inputs

## Behavior Recognition and Threat Analysis

- Human behavior logic, What if Results
- Monitor activity at Bldg X, Retrieve normal 11 am daily activity for building X, compare it to today's activity; if different, try to find some pattern in past like today's: was it a range test?



## Knowledge Base

- Collected and Learned Knowledge
- Buildings, Routes, Personnel, Functions
- Security Device Types, Location and Function
- Surveyed and learned activity, daily, weekly, monthly, etc

## Situational Awareness and Data Display



**Response Control**  
Alerts and Notices  
EO/IR, Counterintelligence,  
Virtual Presence, Broad  
Area Surveillance



## Land point or small area

Point sensors (geophone, vibration, electromagnetic)  
Millimeter and Microwave radar systems  
Video (infrared, image intensified, visible)  
Active pan/tilt/zoom control, cued searches, object tracking, event detection triggers

## Land Perimeter

Strain-sensitive cable, ported coaxial cable, microwave fence, buried lines (seismic, magnetic), optical beam,

## Marine Surveillance Systems

EO/IR, UW Acoustics, radar, ladar,



RFID Tag



License Plate Reader

## Visitor Control/ Access Systems

Biometrics, Badges, Face Recognition  
Portals, Vehicle/Cargo Screening Systems



HumanID



Port Allen/PMRF Beach

PMRF

Makaha Ridge/Kokee Park



## Backup Slides

- Backup Slides Follow



## Base Survey - Notional Assets

- Notional Assets that can be “staged” at PMRF
  - Operations Facilities
  - R&D Facilities
  - Mission/Test Facilities
  - Airfields/Flight Lines
  - Communications Resources
  - Radar/Sensor Installations
  - Ammunition Storage
  - Fuel Storage
  - Troop/Crew Quarters
  - Military Housing
  - Guest Housing
  - Schools/Child-Care
  - Entertainment/Sports Facilities
  - Water Supply
  - Power Plant
  - Port Facility





- Cardinal Scenarios
  - Scenario 1, VBIED + Hostage
  - Scenario 2, Suicide Bomber
  - Scenario 3, Insider Theft
  - Scenario 4, Vandalism and Mission Event Disruption
  - Scenario 5, Stealthy ED/CB
- Annotate with Behaviors, Observables and Measures of Effectiveness (MOE)
- SBOM form the foundation for the agent-based model



## PBPL SBT Key Elements

- The Base buildings, roads, boundaries and facilities are represented by a simple 2D map (obfuscated to avoid compromising base security).
- Agents represent moving objects (people, vehicles, etc.) and security technologies (sensors) placed on the map. Agents emulate the behavior or effect of the objects they represent
- Scenarios are scripted movements of non-threat (civilian) and threat (intruder) agents around and on the base. These agents emit observable behaviors.
- Security Solutions are layouts of security technologies (sensors) that can detect certain observable behaviors within a specified coverage area with a specific probability of detection and false alarm rate.
- An Excursion is a 1-1 combination of a specific scenario and a specific security solution.
- A Replicant is an executable simulation of an excursion with a specific random number seed.
- When a replicant is run, a log is generated of all of the behaviors emitted by agents as they move across the base. Another log is generated of behaviors detected by sensors based upon their coverage area, probability of detection and the random seed.
- A data distribution can be generated for an excursion using variations on the security solution and multiple replicants. This can provide insight into the efficacy of the security solution for the given scenario.
- You can use the same security solution in multiple excursions (e.g. paired with a variety of different scenarios) to understand the overall performance of your security solution.



## PBPL SBT Data Farming

- Use Design of Experiments to focus on the most significant parameters to investigate.
- Use the batch mode of PFPL SBT to run a large number of variations and replicants on an excursion. Also run a significant number of excursions. Yield multiple thousands of data points.
- Plot the Measures of Effectiveness for the security solutions across a number of scenarios and look for trends.
- Plot the cost factors for the security solutions and look for trends.



## Cost-Benefit Analysis

- Each sensor/security technology can be assigned the following cost factors:
  - Fixed Costs: Unit Cost, Bandwidth, CPU, Storage (Total is calculated)
  - Recurring Costs: Recurring Unit Cost, Maintenance, Operational, Training (Total is calculated)
- Create multiple excursions pairing the same scenario with different solutions
- Plot the excursions to compare cost and performance



## Effects Analysis – Prioritized Behaviors

### *Primary Effects*

- TAMPERING\_WITH\_OBJECT
- DAMAGING\_DESTROYING\_OBJECT
- DISCARDING\_ETAG
- DIVERGING\_FROM\_ROUTE
- CARRYING\_WEAPON
- CARRYING\_FIREARM
- INITIATING\_FALSE\_ALARM
- ATTEMPTING\_UNAUTHORISED\_ENTRY
- MAKING\_UNAUTHORIZED\_ENTRY
- SETTING\_FIRE\_TO\_OBJECT
- BREACHING\_FENCE
- FAMILIAR\_HOSTILE
- CARRYING\_EXPLOSIVES
- CARRYING\_WMD

### *Secondary Effects*

- MOVING\_ERRATICALLY
- VEHICLE\_SPEEDING
- MOVING\_EXCESSIVELY\_FAST
- VICINITY\_RESTRICTED\_OBJECT
- CARRYING\_STOLEN\_ID
- VEHICLE\_EXCESSIVELY\_HEAVY
- INITIATING\_FALSE\_ALARM
- OPENING\_UNLOCKED\_DOOR
- DIVERGING\_FROM\_ROUTE

### *Tertiary Effects*

- RUNNING
- LOITERING
- CIRCLING
- MOVING\_BACK\_AND\_FORTH
- VICINITY\_LOCKED\_DOOR
- BEHAVING\_NERVOUSLY
- AVOIDING\_PORTAL
- UNUSUAL\_ARRIVAL\_TIME
- APPROACHING\_FENCE
- VICINITY\_FENCE
- VICINITY\_PORTAL
- APPROACHING\_PORTAL
- ENTERING\_PORTAL
- OPERATING\_RENTAL\_VEHICLE
- UNFAMILIAR\_PERSON

### *Quaternary Effects*

- PRESENT
- ALONE
- IN\_GROUP
- WALKING
- DRIVING
- STATIONARY
- STOP\_MOVING
- START\_MOVING
- JOINING\_GROUP
- LEAVING\_GROUP
- ATTAINED\_GOAL
- CARRYING\_PASS
- CARRYING\_OTHER\_ID
- CARRYING\_ETAG





## Baseline Architecture Details – Use Cases

- The system gathers information about the prevailing state of affairs.
  - Sensors continuously monitor different areas of the base.
  - Agents periodically access external data sources over the network.
  - A Web site accepts inputs from humans.
- An operator monitors the state of affairs on a situational awareness display. The situational awareness display is a geographic rendering of the area. The rendering includes static objects such as buildings as well as detected objects of interest such as people and vehicles. Detected objects are displayed in real-time. The operator has the ability to zoom into areas of interest.
- Information gathered by the system is fused into a common set of tracks. In other words, different information referring to the same object is fused to form a single object instance.
- Behaviors are formulated by analyzing the fused tracks.
- Over time, the system learns what sort of behaviors are to be expected.
- Threat analysis is performed by comparing the currently observed behaviors with the sorts of behaviors that are expected. The threat analysis may request other data from local or remote databases to better determine the state of affairs.
- Unexpected behaviors create an alert to the operator. The alert includes a threat level and a location of the alert on the situational awareness display. Alert thresholds will be able to be adjusted for normal activity versus during an exercise or visit by a dignitary.
- The operator can review information leading up to the reported alert. The information may be a single event or a series of events. The information presented will include the time, date and location of the event. The operator will be able to drill down into all available information including threat level, snapshots and resolution logs.
- The operator indicates to the system whether or not the alert is warranted.
  - If the alert is not warranted, the system may ask the operator to input additional information so that it can learn more about the situation.
  - If the alert is warranted, the system may suggest an investigative course of action based on the current state of security assets.
- Following each investigative action, a description of what was done and the outcomes are entered into the system to support subsequent analysis.



## Baseline Architecture Details – Development Use Cases

- The PFPL project is an R&D effort. It is therefore important to consider the use cases for the development phases of the project as follows:
  - The development of the system will be executed by a number of contractors working on different functional areas such as sensors, behavior recognition, displays and threat analysis.
  - Researchers view the architecture as the framework through which they can effectively contribute to the construction of a semi-autonomous system that improves itself with experience.
  - Developers use the architecture to identify framework components that are of practical importance to their implementations, and to design appropriate extensions, additions or other modifications.
  - Contractors may be developing the identical functional capability with different approaches that need to be evaluated.
  - Various configurations of sensors and functional components must be easily constructed, integrated and tested.
  - Spiral builds will be released on at least an annual basis.
  - Experimentation information will be shared with researchers on and off site.



## Baseline Architecture Details – Top Level Requirements

- The architecture shall be modular. It is expected that multiple contractors will be developing parts of the system in parallel. Functional partitioning of the system into functional modules with well-defined interfaces shall be essential to the realization of this requirement.
- The architecture shall be extensible. The addition of sensors and algorithms over time requires extensibility not only in the addition of new sensors but also recognition of diverse behaviors that may be unforeseen in the initial development. New algorithms to process these behaviors will also be developed over time.
- The architecture shall support experimentation. The architecture must support a rapid prototyping environment where configurations of sensors and algorithms can be rapidly generated and evaluated. The architecture also needs to support testing for integration and evaluation.
- The architecture shall be real-time. A continuous flow of new information must be processed without significant backlog. The latency requirements are those imposed by human reaction time (seconds).



## Baseline Architecture Details - Inputs

- Sensors
  - Sensor information shall take the form of raw data such as video or shall be processed information that may provide information such as the position of an object of interest.
- Sensor Interface
  - The sensors feed the system through a common sensor interface that merges all sensor input into a common data stream. This interface will allow seamless incorporation of sensor suites.
- Data Fusion
  - The data fusion function shall take information from the various sources and associate them to form tracks. These tracks will form the basis of monitoring all objects within the system. Data fusion at the earliest stages of detection allows the same object detected by different sensors to be associated with a single track. Data from external sources will also be associated to tracks by the data fusion function.
- External Data
  - External data comes primarily from available databases such as visitor entry logs or sources outside of the base such as criminal record databases. External data may also be entered by the operator or through a Web site (e.g. an event reported wirelessly by a guard). External data may be continuously updated or may be requested when required.



## Baseline Architecture Details - Repositories

- Data Repository
  - The data repository shall maintain a cache of the recent history for processing as well as long term history for display. Client functions shall have the ability to update information in the cache and request notification when information is changed. The amount of history stored in the data repository shall be a function of a specified maximum time as well as the constraints of the storage media.
- Knowledge Base
  - The architecture shall support the use of ontologies by maintaining descriptions of their properties, interrelationships and conditions under which they are appropriate. Like other types of software, the ontologies will evolve as the system matures. Initially an upper ontology will be developed for the project domain that overarches a family of lower metaphorical ontologies. Relationships spanning lower ontological concepts will be defined to support collective reasoning among agents that employ different viewpoints. As new approaches to implementing reasoning are introduced, or additional useful viewpoints are derived, the ontology catalog will be expanded accordingly.



## Baseline Architecture Details – Cognitive Architecture

- Behavior Recognition
  - The behavior recognition function shall train itself through continuous track observation. It will reason about the observed properties of tracked objects in the context of knowledge it has already acquired regarding normal base activities. The behavior recognition function shall be comprised of a collection of functions that reason cooperatively from different viewpoints. Over time, these functions will develop an understanding of routine base activities and learn to expect certain types of behaviors to be observed in certain places at certain times. Deviations from these expectations form the basis of threat assessments. Behavior interpretations will be made available to operators in a form that they can easily understand.
- Threat Analysis
  - The threat analysis function shall monitor recognized behaviors associated with tracks over time. Tracks that are unable to be associated with recognized behaviors, or that are associated with unexpected behaviors, shall be considered to be an indication of a potentially threatening incident. Individual incidents may not warrant attention but a series of events over a period of days or months may be an indication of an impending undesirable event. An impending undesirable event will generate an operator alert. The threshold of alerts shall be based upon a parameter set by the operator.
- Agents for Reasoning and Learning
  - The behavior recognition and threat analysis functions shall be comprised of reasoning agents. The software architecture shall accommodate various approaches to implementing learning and reasoning, and shall provide suitable hypothesis and belief spaces within the data repository for reasoning agents to share. Tracks, hypotheses and beliefs will be associable such that queries can return elements from one or all categories.
- Reasoning Visualization
  - Reasoning visualization allows for an operator to investigate the chain of reasoning which led to a particular conclusion. It also supports human-directed learning where operators “teach” the system when something is normal and when it is not.





## Baseline Architecture Details – Outputs

- Situational Awareness
  - The situational awareness function shall provide the operator with views of the current and historical state of the monitored areas. The operator shall have the ability to visualize all activity in the monitored area and zoom into areas of interest. This function shall also provide the alerts of impending undesirable events. The operator indication shall take the form of a DEFCON level from 1 to 5 as well as alerts to specific events of interest.
- Response Control
  - The response control function shall monitor the state of the security assets such as patrols. The response to the action shall be saved with the event to for subsequent use by the behavior recognition function. Action response information will help teach the system how to better interpret behaviors in the context of future conditions on the base.
- Raw Data Display
  - The display of raw data is extracted into its own module to allow the process to be replicated and distributed across multiple processors.
- Data Collaboration
  - The data collaboration function shall archive experimental results and post the results to be shared by researchers. The data shall be in both machine and human readable forms. The information shall include data collected as a part of the run as well as text and graphics that analyze the performance results. The data collaboration module extracts experimentation data, formats the data and posts the data on private portal accessible over the Internet.